Commonwealth of Massachusetts
Information Technology Division

Enterprise Wireless Security Standards: Wireless Wide Area Networks Version 1.0

This document identifies standards to ensure secure deployment, use and administration of Wireless Wide Area Networks (WWAN) by Commonwealth entities. Entities considering deployment of these technologies should first consult the Enterprise Wireless Security Policy. Entities covered by this policy must adhere to the standards detailed in this document for all WWAN deployments.

This document is one of the following Enterprise Wireless Security Standards documents that address major categories of wireless technology implementation:

- Wireless Wide Area Networks (WWAN)
- Wireless Local Area Networks (WLAN)
- Wireless Mobile Communications (WMC)
- Wireless Personal Area Networks (WPAN)

Wireless Wide Area Networks (WWAN)

Wireless WANs are defined as radio systems operating within licensed FCC regulated frequencies installed for building-to-building communication between edge devices (i.e., routers) which are usually connected to a wired network, but can be an intermediary hop or aggregation point within the wireless network.

One basic tenet of fixed wireless technology is the requirement for “line of sight.” The transmitting and receiving antennas communicate through a relatively narrow radio frequency (RF) beam. This directional point-to-point RF approach is in stark contrast to the omni-directional antennas used in “mobile” or “WiFi” environments where anyone in the vicinity can receive the signal. With fixed wireless, only an antenna firmly in the focused RF target area can receive the signal. Mac address registering and data encoding insure additional security. Potential intruders would need to obtain the unique Mac address of a radio and the data transmission code sequence being utilized, assuming they had been able to intercept the RF signal and obtain a device capable of utilizing the licensed frequency, to begin “stealing” packets. These aspects of point-to-point wireless technology minimize the opportunity for intrusion.

Typical microwave devices include a radio, dish (or possibly a directional antenna for short range communication), channel bank and a router (or layer 3 switch) for connectivity to the “wired” network. The protocol(s) used by the radios can vary, but most utilize the same digital signaling as (wired) leased lines (e.g. T1/E1/DS1 – T3/E3/DS3, Sonnet, etc.). Newer hardware can provide a direct IP path utilizing Ethernet (802.3) standards.

Enhanced Security Options

Third party products can be added to further encrypt the data stream. Such a device can provide multiple levels of encryption with, at minimum, a 56-bit key. Configurations including such products require a device at each end of the link to affect the data portion of the packets.

1. Infrastructure Standards (WWAN)

A. Registration of radio & tower locations and type (dish/antenna)
Commonwealth entities will assign specific responsibility for the creation and maintenance of a list identifying all WWAN connection points.

B. Use of only devices that operate in FCC licensed frequencies
Entities will apply for and receive FCC licensure prior to installing a fixed WWAN device and will maintain a list of all frequencies they have been license to utilize.

C. Physical security of radios
Radios must be installed securely and lock-boxes are required in locations that are publicly accessible.

D. Separation of wireless and wired networks
WWANs will be separated from the wired network by a firewall or edge device with integrated firewall support wherever possible.

E. Minimal IP scheme
Edge devices will be configured with variable-length subnets of 2-addresses, whenever possible, to further help prevention/intrusion detection.

F. Ensuring network availability, reliability and support
Entities will develop a policy to ensure network availability and reliability for high-priority traffic. Entities or their network providers should establish requirements for Help Desk and support coverage (e.g., 24x7), maximum time to response for service calls, service reliability (e.g., MTBF), network coverage, and maintenance of software and equipment at current firmware/software revision levels.

G. Monitor network security and performance
Entities should effectively manage their wireless connections, including monitoring wireless traffic, devices and potential security risks. Intrusion detection/prevention capability is recommended for complex networks.

2. Authentication Standards (WWAN)

A. No direct user access
Entities will only utilize fixed wireless WWANs for building-to-building communication. Individual user access is not supported.

B. No unauthenticated access allowed on WAN/MAGNet
Unauthenticated public access is not allowed on the Commonwealth WAN or MAGNet network. Any WWAN that allows unauthenticated access must be separated from the WAN/MAGNet and treated as a separate DMZ external to the secure network; any access to the WAN/MAGNet from such a network must comply with the Commonwealth's Enterprise Remote Access Security Policy published by ITD.

C. Encryption within applications required
Entities must be aware that outward facing applications (e.g., customer and vendor programs) may be running across insecure wireless networks at the customer or vendor site; entities must design such applications to enforce data security through encryption at the application level (for example, SSL 128-bit encryption within browser for e-mail, or SSL web interface to customer facing systems). All such applications, whether for PC, PDA, SmartPhone, must support Internet browsers with a minimum SSL128-bit encryption (or equivalent for non-web applications).

D. Local caching, storing and printing
Entities must be aware that local storing, caching or printing of confidential data as defined by the entity on remote devices may pose a significant data security risk. Entities must advise users that confidential data cannot be stored on the devices unless strongly encrypted. Entities should develop local policy as required to address this potential risk, in compliance with the Commonwealth's Enterprise security policies as published by ITD, HIPAA, FIPA, FERPA and relevant data confidentiality acts.

3. Encryption Standards (WWAN)

Entities should develop an encryption policy as required in compliance with the Commonwealth's enterprise security policies as published by ITD, and relevant data confidentiality acts such as HIPAA, FIPA, FERPA, based on the type of data involved..

4. Device Configuration and Security Standards (WWAN)

A. Protection of connected devices
All devices that connect to the Commonwealth LAN/MAGNet via wireless WANs must be configured in compliance with the Commonwealth's Enterprise security policies. Devices must be fully updated and patched, and must run personal firewall and anti-virus software, if available for the device – whenever possible managed by the entity and not the user -- in compliance with Commonwealth and entity policies.

B. Ownership of connected devices
All WWAN devices that connect directly or indirectly to the Commonwealth LAN/MAGNet must be the property of the Commonwealth. No personally owned Wireless Wide Area Network communications devices or vendor equipment may connect without express written permission of the Executive Department CIO, subsequent to a recommendation from the Enterprise Security Board. Commonwealth entities may apply for variances to this ownership requirement on an application-specific basis.

All users of WWAN connected devices must complete and sign a user acceptance agreement, similar to current VPN user acknowledgement, allowing ITD and their entity to scan/monitor and periodically audit the device. The user acknowledgement form must state that no one other than the authenticated user can use the device. Users of non Commonwealth-owned devices who have been approved for such use by the Executive Department CIO must complete the same user agreement noted above.

C. No connection to non-entity networks
No Commonwealth entity's wireless device may be utilized to connect to a non-entity controlled network unless authorized by the entity and ITD.